Privacy Impact Assessment

for the

Data Analysis & Research for Trade Transparency System

DHS Reference No. DHS/ICE/PIA-038(a)

April 11, 2023

Homeland Security

Abstract

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) has deployed an information system called the Data Analysis & Research for Trade Transparency System (DARTTS), which is a component system of HSI's larger Repository for Analytics in a Virtualized Environment (RAVEN) platform. DARTTS analyzes trade data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes. This system will replace a similar system currently in use by HSI, called FALCON-DARTTS, which had the same purpose and functionalities, but resided on a vendor-owned operating platform named FALCON. This Privacy Impact Assessment (PIA) update is necessary to provide public notice of the existence of DARTTS within RAVEN and that the legacy FALCON-DARTTS system will be retired.

Overview

RAVEN DARTTS has been developed for the HSI Trade Transparency Unit (TTU). Trade transparency is the concept of examining U.S. and foreign trade data to identify anomalies in patterns of trade. Such anomalies can indicate trade-based money laundering or other import-export crimes that HSI is responsible for investigating, such as smuggling, trafficking counterfeit merchandise, the fraudulent misclassification of merchandise, and the over- or under-valuation of merchandise for purposes of commercial fraud. HSI uses DARTTS to conduct trade transparency analysis to identify and investigate these illegal activities. As part of the investigative process, HSI investigators and analysts must understand the relationship between importers, exporters, and financing for trade transactions. Examining these transactions allows HSI personnel to determine which transactions are suspicious and warrant investigation. If performed manually, this process would involve hours of analysis of voluminous data. DARTTS is designed specifically to make this investigative process more efficient by automating the analysis and identification of anomalies for the investigator.

DARTTS allows investigators to search and filter details for imports or exports on any number of variables, such as country of origin, importer name, manufacturer name, and total value. DARTTS is not used to predict future behavior or "profile" individuals or entities (i.e., identify individuals or entities that meet a certain pattern of behavior that has been pre-determined to be suspect). Instead, DARTTS identifies trade transactions that are statistically anomalous based on user-specified queries. If HSI determines an anomalous transaction identified by DARTTS warrants further investigation, HSI personnel will gather additional corroborating facts, verify the accuracy of the DARTTS data, and use their judgment and experience in deciding whether to investigate further.

Reason for the PIA Update

HSI is transitioning its analytical processes away from a vendor-owned cloud platform, called FALCON, into its in-house solution, named RAVEN.[1] RAVEN is a cloud-based platform that enables HSI users, who are law enforcement officers or support law enforcement, to perform analytics across raw or unevaluated datasets using a suite of search, analytical, and reporting tools. It is specifically designed to combine and maximize the efficiency and capabilities of its tools. RAVEN leverages capabilities from its set of tools so that HSI programs/divisions may employ RAVEN for multiple tasks, thereby reducing duplication of effort across HSI. In this instance, RAVEN will host DARTTS analytical capabilities and datasets. DARTTS within RAVEN will have the same features and functionality as FALCON-DARTTS with an updated, modern interface to assist with usability. DARTTS within RAVEN's collection, use, maintenance, and dissemination of trade data is consistent with FALCON-DARTTS. A subset of FinCEN data will be available in DARTTS; however, financial data which was previously imported into FALCON-DARTTS will be accessible only through RAVEN's CORE tool.[2]

RAVEN-DARTTS Data, Access, and Storage

DARTTS is used by HSI Special Agents, analysts, and cleared support personnel who work on HSI Trade Transparency Unit investigations at ICE Headquarters and in the HSI field and foreign attaché offices. In addition, select U.S. Customs and Border Protection (CBP) personnel and foreign government partners have limited access to DARTTS. CBP customs officers and import specialists, in furtherance of CBP's mission, use the trade data within DARTTS to identify anomalous transactions that may indicate violations of U.S. trade laws. Foreign government partners that have established trade transparency units and have entered into a Customs Mutual Assistance Agreement (CMAA) or other similar information sharing agreements with the United States have access to certain data in DARTTS and use specific trade datasets to investigate trade transactions, conduct analysis, and generate reports in DARTTS. All HSI, CBP, and foreign government users of DARTTS are only able to access data that is associated with the user's specific profile and associated access permissions.

Trade data is stored in a logically separate data subsystem from the general RAVEN data store, due to its high volume and security controls applicable to foreign government users.[3]

---

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE REPOSITORY FOR ANALYTICS IN A VIRTUALIZED ENVIRONMENT (RAVEN), DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

[2] For more information on RAVEN's CORE tool, please *see* Appendix B of U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE REPOSITORY FOR ANALYTICS IN A VIRTUALIZED ENVIRONMENT (RAVEN), DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

[3] For more information about the types of information RAVEN stores, please *see* U.S. DEPARTMENT OF HOMELAND

Through enhanced RAVEN security controls, HSI and CBP users are granted access to all U.S. and foreign trade data, and foreign government users are granted access to select trade datasets. Foreign government users can use the analytical tools available in DARTTS to analyze trade data, without creating a risk of unauthorized access to data outside the limits of their agreements.

FALCON-DARTTS had a technical limitation that placed a download restriction on all users, thus limiting the amount of information that could be exported from DARTTS. The data download restrictions help minimize the risk that a user could extract excessive bulk data from FALCON-DARTTS without justification. That technical limitation is not present on the RAVEN platform, allowing users to download the data needed for an analysis without a ceiling on data download. However, supervisors have the authority to review the justification for any bulk download, including excessive and/or anomalous downloads. Further, user activity is logged in DARTTS, which can be used to identify normal and anomalous behavioral patterns over time. HSI audits system logs (monthly or as often as deemed appropriate) to determine if any anomalous activity warrants an investigation.

Segregation of non-trade data outside the DARTTS environment

The primary function of DARTTS has always been to work with trade data (imports and exports), for the United States and other partner countries. Over time however, FALCON-DARTTS allowed users to store and view other types of data, such as U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) financial data, user-imported bank transactions, user-imported money services business data, and law enforcement records (e.g., TECS records,[4] and the Specially Designated Nationals list[5]).[6] FALCON-DARTTS also allowed for ad hoc uploads by users to pair with DARTTS data for analysis. For example, pursuant to an administrative customs summons, HSI investigators may have obtained financial records from a bank associated with a shipment of goods imported into a free trade zone and then uploaded those records into FALCON-DARTTS for comparison against trade records.

The DARTTS system within RAVEN will be used for storing and analyzing trade data and a subset of FinCEN data will continue to be available. Other financial data (such as FinCEN),[7] law

---

SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE REPOSITORY FOR ANALYTICS IN A VIRTUALIZED ENVIRONMENT (RAVEN) DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS), DHS/CBP/PIA-009, *available at* https://www.dhs.gov/privacy-documents-cbp.

[5] *See* U.S. DEPARTMENT OF TREASURY, OFFICE OF FOREIGN ACCESS CONTROL, PRIVACY IMPACT ASSESSMENT FOR CONSOLIDATED TECHNOLOGY SYSTEMS, *available at* https://home.treasury.gov/system/files/236/pia_ofac_octs.pdf.

[6] For more information on the types of data previously stored by FALCON-DARTTS, *see* DHS/ICE/PIA-038 FALCON-DARTTS, *available at* https://www.dhs.gov/privacy-documents-ice.

[7] *See* U.S. DEPARTMENT OF TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, PRIVACY IMPACT

enforcement records, or other ad hoc uploads, will be stored separately in RAVEN and accessible through RAVEN CORE.[8] HSI personnel with the need to combine DARTTS data with other data may access the trade data originating from DARTTS through RAVEN CORE. Access to trade data through RAVEN CORE, however, will be limited to users who have also been granted access privileges to DARTTS.

Interaction with RAVEN CORE

RAVEN CORE is the main search and analytic tool for all RAVEN data and any additional future data holdings that HSI will acquire. RAVEN CORE allows users to customize their investigative or analytical workflow by displaying search results from multiple disparate data sources in one workspace, called a canvas. Within the canvas, users can build out and analyze criminal networks and associations; and create maps, charts, timelines, and graphs. Users will be able to sort, filter, group, and compare search results from multiple RAVEN datasets; discover relationships; and identify evidence relevant to criminal investigations.[9]

Prior to the development of RAVEN, HSI used the FALCON-Search and Analysis system[10] to search and analyze data ingested from ICE, DHS, and other government data systems and applications. This included DARTTS datasets. The DARTTS system within RAVEN will be used for storing and analyzing trade data and a subset of FinCEN data. RAVEN CORE is designed as a more effective and robust tool to better enable investigators and analysts to store, analyze, and collaborate between different HSI data holdings and external partner databases. RAVEN CORE will replace FALCON-Search and Analysis for creating visualizations of DARTTS data or comparing DARTTS data to other datasets. DARTTS also performs unit price analysis by analyzing trade pricing data to identify over or under pricing of goods, which may be an indicator of trade-based money laundering. The financial data analysis features available previously in the legacy FALCON-DARTTS system will be available in RAVEN CORE after FALCON-DARTTS is retired.

ASSESSMENT FOR CONSOLIDATED TECHNOLOGY SYSTEMS, *available at* https://www.fincen.gov/privacy-impact-assessments.

[8] For more information on the types of data available to CORE, *see* Appendix of U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE REPOSITORY FOR ANALYTICS IN A VIRTUALIZED ENVIRONMENT (RAVEN), DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

[9] As noted previously, HSI personnel gather additional corroborating facts, verify the accuracy of the DARTTS/RAVEN CORE data, and use their judgment and experience in deciding whether to investigate further. Such additional information could include, for example, open source information and other relevant data to which the user has access outside of RAVEN CORE based on their need to access and use such information.

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE FALCON-SEARCH AND ANALYSIS SYSTEM, DHS/ICE/PIA-032, *available at* https://www.dhs.gov/privacy-documents-ice.

Privacy Impact Analysis

Authorities and Other Requirements

There is no change to the legal authorities that authorize DHS's collection and analysis of trade data. DHS is authorized to collect this information pursuant to 19 U.S.C. §§ 1415, 1484, and 2071. HSI has the jurisdiction and authority to investigate violations involving the importation and exportation of merchandise into or out of the United States. Information analyzed by DARTTS supports HSI's investigations into numerous violations, including smuggling under 18 U.S.C. §§ 541, 542, 545, and 554 and money laundering under 18 U.S.C. § 1956.

Notice for the RAVEN environment is provided under DHS/ICE-018 Analytical Records system of records notice (SORN).[11] DARTTS will now fall under that system of records notice for compliance under the Privacy Act of 1974. Records retention for DARTTS is unchanged by the transition to the RAVEN platform. Any records created by DARTTS are governed by N1-567-09-003,[12] which states that records will be destroyed 10 years after cutoff. Any leads created by RAVEN's analytical processes will be retained per evidentiary storage requirements under ICE's Investigative Case Management System (ICM),[13] which is 20 years after case closure in accordance with N1-36-86-1-161.3 (Inv 7b).[14]

HSI does not collect personally identifiable information directly from individuals or enterprises for inclusion in DARTTS, as such the system does not implicate the Paperwork Reduction Act. All information is provided by other government agencies and foreign governments. A complete listing of other U.S. government agency forms and Office of Management and Budget Control numbers can be found in the Appendix of this update (see Appendix, Table 1).

---

[11] *See* DHS/ICE-018 Analytical Records, 86 FR 15246 (March 22, 2021), *available at* https://www.dhs.gov/system-records-notices-sorns.

[12] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-567-093, U.S. DEPARTMENT OF HOMELAND SECURITY, DATA ANALYSIS AND RESEARCH FOR TRADE TRANSPARENCY SYSTEM (DARTTS) (2009), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/n1-567-09-003_sf115.pdf.

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT SYSTEM (ICM), DHS/ICE/PIA-045, *available at* https://www.dhs.gov/privacy-documents-ice.

[14] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-36-86-1-161, U.S. CUSTOMS SERVICE, COMPREHENSIVE AGENCY RECORDS SCHEDULE (1986), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-treasury/rg-0036/n1-036-86-001_sf115.pdf.

Characterization of the Information

There is no change to the types of trade data DARTTS collects or maintains. Other data that was imported into DARTTS (financial data, other ad hoc data[15]), with the exception of a subset of FinCEN data, is now segregated from DARTTS and is only accessible through RAVEN CORE[16] The DARTTS system within RAVEN uses U.S. trade data collected by and received from CBP and foreign trade data collected by and sent to DARTTS from foreign governments.

U.S. Trade Data

(1) CBP Import Data: Import data in the form of extracts from CBP's Automated Commercial Environment (ACE),[17] which CBP collects from individuals and entities importing merchandise into the United States who complete CBP Form 7501 (Entry Summary) or provide electronic manifest information via the Automated Commercial Environment.

(2) CBP Export Data: Export data in the form of Electronic Export Information (EEI)[18] that CBP collects from individuals and entities exporting commodities from the United States.

(3) Bill of Lading Data: Transportation documents collected by CBP via the Automated Commercial Environment[19] and provided to HSI through electronic data transfers for upload into DARTTS.

Foreign Trade Data

(4) Foreign Import and Export Data: Import and export data provided to HSI by foreign government partners pursuant to a Customs Mutual Assistance Agreement or other similar information sharing agreement. Certain countries provide trade data that has been stripped of personally identifiable information. Other countries provide

[15] "Information uploaded on an *ad hoc* basis is obtained from various sources and may include financial records, business records, trade transaction records, and transportation records. For example, pursuant to an administrative customs subpoena, HSI investigators may obtain financial records from a bank associated with a shipment of goods imported into a free trade zone." For more information, see page of 8 of U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE FALCON-SEARCH AND ANALYSIS SYSTEM, DHS/ICE/PIA-032, *available at* https://www.dhs.gov/privacy-documents-ice.

[16] All data ingested or received by RAVEN is listed in Appendix A of DHS/ICE/PIA-055 RAVEN.

[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR AUTOMATED COMMERCIAL ENVIRONMENT (ACE), DHS/CBP/PIA-003(B), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[18] The Electronic Export Information is required documentation when the value of the commodity classified under each individual tracking number is over $2,500 or if a validated export license is required to export the commodity. The exporter is responsible for preparing the Electronic Export Information and the carrier files it with CBP through the Automated Commercial Environment.

[19] A Bill of Lading is a commercially available document issued by a carrier to a shipper, regarding receipt of the goods, the conditions on which transportation is made, and the terms of delivery to the port of destination.

complete trade data, which includes names and other identifying information that may be contained in the trade records.

Foreign trade data is uploaded into DARTTS through a web-based interface. Once the upload is approved by the HSI Trade Transparency Unit, the data is loaded into the DARTTS storage on the RAVEN platform. When the data is loaded into the system, it is tagged so the system knows which country provided it and can identify that data and grant access to that government's users.

All data analyzed by DARTTS is updated on at least a monthly basis for all sources, or as frequently as the source system/country can provide updates or corrected information. A complete listing of source data refresh periods can be found in the Appendix (see Appendix, Table 2).

The data used by DARTTS is assessed to be accurate because the data was collected directly from the individual or entity to whom the data pertains. There are often significant impediments to directly verifying the accuracy of the information with the individual to whom the specific information pertains, as doing so may reveal to the individual that he or she is under investigation. Thus, DARTTS relies on the systems and/or programs performing the original collection to provide accurate data. Users are trained to check anomalous data identified in DARTTS against information from the original data sources prior to generating a lead. Some users have separate access to the DARTTS source databases, as well as other government databases and open source data sources, including social media information. The HSI Trade Transparency Unit validates and approves all trade data that will be uploaded by a user (i.e., Foreign Partner DARTTS user), prior to it being uploaded into DARTTS.

Data utilized in DARTTS is sourced from CBP. CBP validates the accuracy of the data collected directly from exporters and importers by inspecting cargo and accompanying documentation for verification. Electronic information filers must receive training and obtain a certification from CBP before transmitting data. Electronic filers are required to maintain an acceptable level of performance filing timely and accurate information. DARTTS validates each data transmission when authorization is granted for electronic filers. Any inaccurate or incorrect data is removed from DARTTS once identified and accurate and correct data is updated into DARTTS at the soonest opportunity. ICE and CBP are developing additional measures to ensure any inaccurate data discovered in DARTTS, sourced from CBP, will be corrected in the CBP source systems.

Uses of the Information

There is no change to the use of information within DARTTS, or to the user access privileges granted to the data within DARTTS now that it resides within RAVEN. DARTTS is used by HSI personnel, CBP personnel, and foreign government personnel with a verified need to know the information to investigate illicit activity in connection with international trade. There are

no changes to the functionality, capabilities, or analysis conducted by the system, except that a subset of FinCEN data will remain, and the remaining financial data analysis will occur using RAVEN's CORE tool outside DARTTS.

DARTTS assists its users in identifying suspicious trade transactions by identifying and analyzing trade data that is statistically anomalous. Such anomalies can indicate trade-based money laundering or other import-export crimes that HSI is responsible for investigating, such as smuggling. For example, DARTTS allows HSI investigators to view totals for merchandise imports and sort on variables, such as country of origin, importer name, manufacturer name, and total value. DARTTS can also identify links between individuals and/or entities based on commonalities, such as identification numbers, addresses, or other information. Investigators follow up on anomalous transactions or suspicious commonalities to determine whether they are in fact suspicious and warrant further investigation.

HSI Use of DARTTS

HSI users of DARTTS conduct analyses of trade data to identify potential violations of U.S. criminal laws. The analyses are designed to generate leads for and assist with the investigation of trade-based money laundering and smuggling. DARTTS in RAVEN conducts two types of analyses:

(1) International Trade Discrepancy Analysis: U.S. and foreign import/export data is compared to identify anomalies and discrepancies that warrant further investigation for potential fraud or other illegal activity.

(2) Unit Price Analysis: Trade pricing data is analyzed to identify over- or under-valuation of goods, which may be indicative of trade-based money laundering or other import-export crimes.

HSI DARTTS users are trained to verify information received from DARTTS before including it in any analytical report or using it as the basis for any formal law enforcement action, such as arresting an individual for a crime. HSI investigators will fully investigate leads generated by DARTTS analysis before taking action against an individual or entity. To ensure they have the best evidence available to support any case they are building, the investigator must obtain information from all original data sources and further investigate the reason for the anomaly. If the anomaly can be legitimately explained, such as when the anomaly is an administrative error or is part of a legal business process, the investigator has no need to further investigate for criminal violations. Any and all information obtained from DARTTS will be independently verified before it is acted upon or included in an investigative or analytical report.

CBP Use of DARTTS

CBP customs officers and import specialists use DARTTS in support of the CBP mission to enforce U.S. trade laws and to ensure the collection of all lawfully owed revenue from trade activities. Specifically, CBP personnel use DARTTS trade data[20] to identify anomalous transactions that may indicate violations of U.S. trade laws. If HSI elects not to open an investigation into these transactions, CBP may initiate administrative enforcement actions to recover delinquent revenue or penalties. Before initiating a formal administrative action, CBP personnel must gather additional facts, verify the accuracy of the DARTTS data, and use their judgment and experience in making the determination to initiate an administrative enforcement action. Not all anomalous or suspicious transactions identified in DARTTS will lead to CBP administrative actions.

Foreign Government Partner Use of DARTTS

Foreign government users who have access to DARTTS are granted a user role that allows them to use only the trade data provided by their country and related U.S. trade data to investigate trade transactions, conduct analysis, and generate reports. Foreign government users do not have access to the financial and law enforcement datasets or the trade datasets of other partner countries, unless access to other partner countries' data is authorized pursuant to information sharing agreements. Foreign government user access is only granted to foreign government partners that have their own established trade transparency units and have entered into a Customs Mutual Assistance Agreement or other similar information sharing agreement with the United States. Foreign governments do not have the authority to create or modify user accounts or privileges.

Privacy Risk: There is a risk of unauthorized access to the information maintained in DARTTS in RAVEN, and a risk of unauthorized access to data outside of DARTTS (i.e., other RAVEN data) by CBP and foreign government users.

Mitigation: This risk is partially mitigated. DARTTS's security controls are implemented in the RAVEN platform. As an application within RAVEN, DARTTS will possess the same technical, administrative, and physical safeguards as other tools within the RAVEN environment. Data retention and user access is controlled at the record level. Trade data is stored in a logically separate data subsystem from the general RAVEN data store, due to its high volume and security controls necessary for foreign government users. As such, access to RAVEN does not allow an individual access to DARTTS data. Similarly, for foreign government users and CBP users, access to DARTTS data will not allow a user to access other data or tools within RAVEN (e.g., financial data, law enforcement records).

[20] CBP users do not have access to financial datasets.

RAVEN security and access controls are in place to mitigate the risk of unauthorized individuals gaining access to personally identifiable information. RAVEN also has robust logging and auditing controls, which track any user that accesses a record. Audit capabilities log user activities making them available for later query, which allows program managers and system administrators to identify improper export of data. HSI audits access logs and ICE or CBP personnel who are found to access or use the DARTTS data in an unauthorized manner will be disciplined in accordance with DHS policy. Further, foreign government user access is only granted to foreign government partners that have their own established trade transparency units and have entered into a Customs Mutual Assistance Agreement or other similar information sharing agreement with the United States. Foreign government users who access data for non-official purposes are removed from the system and may be subject to disciplinary action by their foreign government employer. Further, any violation of the Customs Mutual Assistance Agreement or other underlying information sharing agreement, including established privacy safeguards, may be grounds for terminating the agreement.

Notice

There is no change to the notice given by DARTTS when transitioned to RAVEN, except that it is now covered by the DHS/ICE-018 Analytical Records system of records notice[21] instead of its previous system of records notice, DHS/ICE-005 Trade Transparency and Research, which has since been retired.[22] The data collected and maintained by RAVEN for DARTTS is outlined in its Privacy Impact Assessment, DHS/ICE-055 RAVEN.[23] This Privacy Impact Assessment provides general notice to the change in platform from the FALCON environment to the RAVEN environment.

Privacy Risk: There is a risk that individuals may be unaware that their information is contained within RAVEN instead of FALCON-DARTTS.

Mitigation: This risk is partially mitigated. Publication of this Privacy Impact Assessment and the DHS/ICE-018 Analytical Records system of records notice provides a detailed description of the types of individuals whose information is contained within the system and the types of trade transactions that make up DARTTS data. Separately, ICE Privacy is also updating the RAVEN Privacy Impact Assessment to provide notice for the ingestion of the DARTTS datasets within its source system appendix. However, because of the nature of the analysis completed within the

[21] *See* DHS/ICE-018 Analytical Records, 86 FR 15246 (March 22, 2021), *available at* https://www.dhs.gov/system-records-notices-sorns.
[22] *See* notice of the retirement of two Privacy Act System of Records Notices, 87 FR 6620 (February 4, 2022), *available at* https://www.dhs.gov/system-records-notices-sorns.
[23] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE REPOSITORY FOR ANALYTICS IN A VIRTUALIZED ENVIRONMENT (RAVEN), DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

system (e.g., identification of suspicious trade transactions), HSI does not provide notice directly to individuals that their data is included in and used in DARTTS.

Data Retention by the Project

The previous FALCON-DARTTS Privacy Impact Assessment stated that ICE intended to request National Archives and Records Administration (NARA) approval to retire the legacy DARTTS records retention schedule and incorporate the retention periods for data maintained in FALCON-DARTTS for 10 years. Records retention for DARTTS is unchanged by the transition to the RAVEN platform. Any records created by DARTTS are governed by N1-567-09-003,[24] which states that records will be destroyed 10 years after cutoff. Any leads created by RAVEN's analytical processes will be retained per evidentiary storage requirements under ICE's Investigative Case Management System, which is 20 years after case closure in accordance with N1-36-86-1-161.3 (Inv 7b).[25]

Data in RAVEN will be refreshed from the source systems at a regular rate. As source system information refreshes, it will delete any data within RAVEN designated for destruction. All data ingests are also tagged with the source system retention schedule, thus even without the system update, records only will be retained for the relevant retention schedule in RAVEN.

All visualizations and analytics products created by RAVEN CORE contain data tags that point to the underlying records in the RAVEN database. Analytical products are considered intermediary records which are destroyed upon verification of successful creation of the final document or file (such as a generated lead), or when no longer needed for a business use, whichever is later. When underlying records are deleted through system refreshes, the analytical product will also be deleted automatically. If analytical products are marked by an analyst or agent as connected to an ongoing investigation or case these products will be transferred to the relevant case management system, which has its own processes for ensuring proper data retention and destruction.

Information Sharing

There are no changes to the policies and procedures for sharing leads generated from DARTTS with external parties. ICE may share final analytical products of RAVEN with law

[24] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-567-093, U.S. DEPARTMENT OF HOMELAND SECURITY, DATA ANALYSIS AND RESEARCH FOR TRADE TRANSPARENCY SYSTEM (DARTTS) (2009), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/n1-567-09-003_sf115.pdf.

[25] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-36-86-1-161, U.S. CUSTOMS SERVICE, COMPREHENSIVE AGENCY RECORDS SCHEDULE (1986), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-treasury/rg-0036/n1-036-86-001_sf115.pdf.

enforcement or intelligence agencies that demonstrate a need to know the information in the performance of their missions and in furtherance of HSI's own law enforcement analyses or investigations. These agencies can include federal, state, tribal, local, and foreign law enforcement agencies. ICE only shares this information after the underlying data has been validated and only for law enforcement or homeland security purposes. This sharing will take place only after ICE determines that the receiving component or agency has a need-to-know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in the DHS/ICE-018 Analytical Records system of records notice and applicable law, regulation, or policy. As DARTTS is now on the RAVEN platform, different technical controls govern external partner access within DARTTS. All data within RAVEN is separated logically, at the record level, through tagging. Every record brought into the system will be assigned one or more attributes, referred to as a "Security Vault" within RAVEN. Users are then granted permissions to view and add records to that Security Vault based on their need-to-know and job duties. As a default, a user's access privileges to a tool or dataset on RAVEN are limited to access he or she has to the source system(s). System administrators or HSI program managers verify personnel's need-to-know before granting access to RAVEN tools or datasets. For DARTTS, need-to-know will be verified by the HSI Trade Transparency Unit prior to granting access to foreign government users.

Access to data within DARTTS is controlled depending on the type of user. Access is limited for foreign partners to the trade data of their country and the related U.S. trade transactions between their country and the United States, unless access to other partner countries' data is authorized via information sharing agreements. DARTTS user roles are configured to ensure that foreign government users access only the select trade datasets they are authorized to view, access, and analyze in the subsystem, with no access beyond that to the other datasets stored in the RAVEN environment or any other internal network resources. Foreign government user access to the logically separate trade data system is filtered through a web application that resides within a protected infrastructure space between the DHS internet perimeter and the DHS/ICE network, accessible only through a secured network connection, thereby protecting the DHS network from unauthorized access.

Privacy Risk: There is a risk that DARTTS data may be disseminated to those without a need-to-know; this risk is exacerbated by removal of technical limitations on large data downloads.

Mitigation: This risk is partially mitigated. DARTTS uses the same access controls, user auditing, and accountability as those described in the RAVEN Privacy Impact Assessment. Audit capabilities log user activities making them available for later query, which allows program managers and system administrators to identify improper export of data. User actions are logged in DARTTS, which can be used to analyze normal and anomalous behavioral patterns. HSI audits

system logs (monthly or as often as deemed appropriate) to determine if anomalous activity warrants an investigation.

Moreover, DARTTS is configured to ensure that foreign government users access only the select trade datasets they are authorized to view, access, and analyze in the system, with no access to other data stored in the RAVEN environment or any other internal network resources. Foreign access to the logically separate trade data system is filtered through a web application that resides within a protected infrastructure space between the DHS internet perimeter and the DHS/ICE network, accessible only through a secured network connection.

Redress

There are no changes to access or redress for individuals seeking their information within DARTTS now that it has transitioned to RAVEN. Individuals seeking notification of and access to any of the records covered by this PIA may submit a request in writing to the ICE Freedom of Information Act (FOIA) Officer by mail or facsimile:

U.S. Immigration and Customs Enforcement Freedom of Information Act Office
500 12th Street SW, Stop 5009 Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

All or some of the requested information may be exempt from access pursuant to the Privacy Act or the Freedom of Information Act (for those individuals who are not U.S. citizens or lawful permanent residents and whose records are not covered by the Judicial Redress Act) to prevent harm to law enforcement investigations or interests. Providing individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

Auditing and Accountability

All auditing and accountability for DARTTS will now be performed by the RAVEN platform. Access is granted on a case-by-case basis by system administrators. User roles are assigned to give users the appropriate access and users who no longer require access are removed from the access list. All HSI, CBP, and foreign government users of DARTTS access only data that is associated with the user's specific profile and role.

HSI Special Agents and Criminal Analysts have an inherent job-related need-to-know use of DARTTS and are assigned user roles for U.S. and foreign trade data.

CBP personnel and individuals assigned to HSI to serve on a task force or from other agencies, must have their supervisor validate that the employee has a job-related need-to-know,

and the appropriate level of background check. For contractors, a government employee overseeing the contract will validate the need to know and perform the other supervisory roles above.

Foreign government users, who are granted access to only select trade datasets stored in the DARTTS trade data subsystem with no access to the other data stored in the RAVEN environment, are vetted by the ICE attaché office in the foreign government user's country before they are considered for access to the subsystem. User accounts are approved by the system administrator. Foreign governments do not have the authority to create or modify user accounts or privileges.

RAVEN implements auditing of user actions in the system. User actions are recorded and stored in audit logs accessible only to authorized personnel. User auditing captures the following activities: logon and logoff, search query strings, records viewed by the user, changes in access permissions, records/reports extracted from the system, and records/reports printed by the system. The system also keeps a complete record of all additions, modifications, and deletions of information in the system and the date, time, and user who performed the action. This information is readily accessible by system administrators and ICE IT security personnel.

Any new uses or sharing of information for RAVEN will be approved by the HSI Trade Transparency Unit and RAVEN system administrators. The existence of this governance process will help to ensure that new data sources are appropriately vetted. Any new sharing of information will require an interconnection agreement with RAVEN and, as appropriate, an update to RAVEN's privacy compliance documentation. Prior to ingestion of any new data source, RAVEN system administrators will confer with the HSI Trade Transparency Unit to determine which users may have access to the new dataset, as well as assess whether an update is required to RAVEN's privacy compliance documentation.

Privacy Risk: There is a risk that DARTTS users may use DARTTS outside the purposes of this Privacy Impact Assessment.

Mitigation: This risk is partially mitigated. DARTTS system administrators perform audits of the system during their management activities of DARTTS. Management activities can include managing accounts and access, reviewing system logs, and receiving feedback from the HSI Trade Transparency Unit regarding their case reviews and approval of user uploaded data. RAVEN system administrators and developers, however, are working to develop further safeguards. System administrators will monitor use of DARTTS over time to determine what will be considered "normal" use of the system and develop flags that indicate use in contravention with the purposes outlined in this Privacy Impact Assessment. This Privacy Impact Assessment will be updated as appropriate to reflect new auditing capabilities and requirements.

Responsible Official

Amber Smith
Deputy Assistant Director
Office of Information Governance and Privacy
U.S. Immigration & Customs Enforcement
Department of Homeland Security
(202) 732-3000

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Mason C. Clutter
Acting Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

APPENDIX

Table 1. Trade Data Transactions Forms

Form	OMB Control No.
U.S. Customs and Border Protection Form 7501 – Entry Summary	1651-0022
Electronic Export Information filed electronically through the Automated Export System (AES)	0607-0152
Cargo inventory and carrier manifest information filed electronically through the Automated Commercial Environment (ACE)	1651-0001

Table 2. Source Data and Refresh periods

Sources of Information	System of Record Notice	Data Refresh
Automated Commercial Environment	DHS/CBP-001 Import Information System, 81 FR 48826, (July 26, 2016)	Daily
Foreign Government Partners	N/A	Monthly